Regn. No. | | | | | | | | | |

MANIPAL INSTITUTE OF TECHNOLOGY

MANIPAL

(A constituent unit of MAHE, Manipal)

II SEMESTER M.TECH (COMPUTER SCIENCE AND INFORMATION SECURITY)
DEGREE EXAMINATIONS, APRIL-2019
SUBJECT : INTRUSION DETECTION SYSTEMS(CSE 5250)
REVISED CREDIT SYSTEM
DATE: 04-05-2019

TIME:03 HOURS MAX.MARKS : 50

Instructions to Candidates:

- Answer ALL FIVE FULL questions.
- Missing data, if any, may be suitably assumed.

1A.	What are the five security goals for Audit Mechanisms as outlined in Rainbow Series	3M
1B.	List and Define the Security Triad.	3M
1C.	Explain Misuse Detection and Anomaly Detection with a Neat Diagram of Generic Intrusion Detection System.	4M
2A.	Explain Non-Parametric Statistical measures in performing Anomaly Detection.	3M
2B.	Explain different Passive Response types in Intrusion Detection Systems.	3M
2C.	Explain the processes involved in behavior classification engine for Anomaly Detection with an example of Intrusion Detecction Expert Systems(IDES).	4M
3A.	List and explain Goals and Objectives of Intrusion Detection System User in an organization.	3M
3B.	What are the common requirements and constraints that might affect the selection of an intrusion detection system?	3M
3C.	Explain the process involved in mapping security policy to configurations by users of IDS with suitable example.	4M
4A.	Explain the following different approaches to security by Designers of IDS. (i) Security as a Control Function (ii) Security as a Risk Management (iii) Security as Ecology	3M
4B.	Explain how changes in Network Fabric and Open Source software will drive future trends in IDS Technology?	3M
4C.	List and explain different Security Design Principles.	4M

5A. Explain the Security Process.How do you express risk with a risk equation? 3M

5B. What is a Defensible Network? What are the different techniques used to control the defensible Network? 3M

5C. What are the Four Network Security Monitoring Data Types to Detect and Respond to incidents? Explain with a network diagram. 4M